bigstep®

Security Overview

Peace of mind. Built right in.

It's critical to efficiently secure systems, facilities, and customer data to protect sensitive corporate and end-customer information from internal and external threats, so we always put security first.

The unique design of our platform allows partitioning and single-tenant control that are not possible in most public cloud environments.

With Bigstep, you get:

- Full Hardware & Software Isolation
- Extension of Enterprise-Specific Security
- Secure Platform Design
- Best Practices & HR Security Management
- Industry Security Certifications
- GDPR Compliance

Bigstep Product Features

- Single-tenant, isolated, bare metal servers – The server hardware is not shared, eliminating security risks associated with multi-tenant, virtualized environments.
- Software-defined Private L2 Network – Security-wise, it is identical to having a switch and cables connected to servers.
- Encrypted Block Storage – SAN-based block devices, locally attached SSDs, and disks that behave like local disks, and can be encrypted.

Bigstep Security

- Secure Architecture – We anticipate vulnerabilities such as DNS spoofing, ARP poisoning, impersonation, XSS attacks, reply attacks, and other types of attacks. All credentials are encrypted.
- Routine Penetration Testing – An external audit company checks for vulnerabilities periodically.
- Strict Security Update Policies - Internal systems are updated on a regular basis. Mailing lists are constantly monitored for Zero-day vulnerability. When something critical is detected, we update our systems and notify our customers to do the same.
- Enterprise Network Extension – The L2 network can securely extend an on-premises network into the cloud via encrypted site-to-site VPN. All servers come with an intuitive firewall which is on by default.
- Private Security Policies - After the initial provisioning, root access credentials can be changed, preventing anyone, including Bigstep staff, from accessing systems.

Bigstep HR & Administrative Practices

- Limited Access to Credentials – Only key staff have access to production systems.
- Social Engineering Protection – All personnel is thoroughly trained against the risks and tactics of attacks such as: pretexting, spear phishing, impersonation of a power figure, and more.
- Two-Factor Authentication - We use 2FA for all our internal tools, such as: source code repositories, messaging app, email, front desk systems, and more.

Security Certifications

We want to offer clients the highest level of security, so we make sure we operate in line with industry best practices and management systems.

Bigstep complies with 27001:2013, 27017:2015, 27018:2014, ISO/IEC 20000-1:2011, and ISO/IEC 9001:2015, ensuring that:

- our products suit their purpose;
- security and safety are built into our products and services;
- we continuously improve the quality of our products and services.

Let's take a closer look at what each of the certifications means and how it protects your business from threats, as well as help you comply with regulations and checks from authorities in your industry.

GDPR Compliance

Bigstep is GDPR-compliant in the way data is collected, processed, and stored across our products and services. We implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, such as:

- The pseudonymization and encryption of personal data;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Data Loss Prevention

When it comes to prevention of data loss, alteration, misuse, unauthorized access or unlawful processing of the collected personal data, we are committed to industry best practices.

- We use encryption technology as appropriate;
- We limit the access to the systems on which the personal data is stored;
- We test our website, data centers, systems, and other assets for security vulnerabilities;
- We constantly monitor for possible attacks and vulnerabilities.

For more information, please read our Privacy Notice. All the described measures are backed by our ISO certifications, as described below.

ISO/IEC 27001

ISO/IEC 27001:2013 - Information Security Management System (ISMS)

The ISO/IEC 27001:2013 standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the organization.

ISO/IEC 27017

ISO/IEC 27017:2015 - Security Techniques for Cloud Services

The ISO/IEC 27017:2015 code of practice gives guidelines for information security controls applicable to the provision and use of cloud services.

ISO/IEC 27018

ISO/IEC 27018:2014 - Security Techniques in Public Clouds Acting as PII Processors

The ISO/IEC 27018:2014 code of practice establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

ISO/IEC 20000

ISO/IEC 20000-1:2018 Information Technology - Service Management

The ISO/IEC 20000-1:2018 standard specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve a service management system (SMS).

ISO/IEC 9001

ISO/IEC 9001:2015 - Quality Management Systems

The ISO 9001:2015 standard specifies requirements for an organization's quality management system in order to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements.

HM Government
G-Cloud 10
Supplier

G-Cloud 10 Certification

The G-Cloud certification allows companies to provide services to UK governmental institutions.